SECURITY INCIDENT & EVENT MANAGEMENT POLICY

VARDHAMAN CAPITAL PVT LTD herewith referred as VCPL , is the SEBI registered Stock Broker & Depository Participant. The under-mentioned policy Security incident & event management policy is created by the Compliance Officer and approved by the Board of Directors on 24/10/2022.

INTRODUCTION

VARDHAMAN CAPITAL PVT LTD is responsible for the security and integrity of all data it holds. The company must protect this data using all means necessary by ensuring at all times that incident which could cause damage to the company's assets and reputation is prevented and/or minimized. There are many types of incidents which could affect security:

PURPOSE

Management of security incidents described in this policy requires the company to have clear guidance, policies and procedures in place. Fostering a culture of proactive incident reporting and logging will help reduce the number of security incidents which often go unreported and unnoticed – sometimes, over a long period of time and often without resolution.

The purpose of this policy is to:

- Outline the types of security incidents
- Detail how incidents can and will be dealt with
- Identify responsibilities for reporting and dealing with incident.

THIS POLICY APPLIES TO:

Company's employees, partner agencies, contractors and vendors. All company departments, personnel and systems (including software) dealing with the storing, retrieval and accessing of data

PROCEDURE

The company is clear that all incident are reported to the concerned department's immedtialey and the company has given below the details for identifying, reporting and recording of security incidents. By continually updating and informing company employees, agencies, contractors and vendors an effective communication channels will be developed .The types of Incidents which this policy addresses include but is not limited to:

COMPUTERS LEFT UNLOCKED WHEN UNATTENDED

Users of company computer systems are continually reminded of the importance of locking their computers when not in use or when leaving computers unattended for any length of time. All company employees, partner agencies, contractors and vendors need to ensure they lock their computers appropriately. Discovery of an unlocked computer which is unattended must be reported to IT Department so that corrective measures can be taken.

PASSWORD DISCLOSURES

Unique IDs and account passwords are used to allow an individual access to systems and data. It is imperative that individual passwords are not disclosed to others. If anyone suspects that their or any other user's password has been disclosed whether intentionally, inadvertently or accidentally, the IT Department must be notified to reset the password immediately.

VIRUS WARNINGS/ALERTS

All Desktop, laptop and tablet computers in use across the company have Antivirus (including Anti-Spyware/Malware)... On occasion, an antivirus warning message may appear on the computer screen. The message may indicate that a virus has been detected which could cause loss, theft or damage to company data. It may indicate that the antivirus software may not be able to rectify the problem and so must be reported to the IT department immediately. Any security updates information will be sent by mail if required and done automatically wherever necessary.

MEDIA LOSS

Use of portable media such as CD/DVD, DAT (magnetic tape), USB Flash sticks/HD drives for storing data requires the user to be fully aware of the responsibilities of using such devices. The use of PCs, laptops, tablets and many other portable devices increases the potential for data to be exposed and vulnerable to unauthorized access. Any authorized user of a portable device who has misplaced or suspects damage, theft whether intentional or accidental of any portable media must report to the IT Department immediately.

DATA LOSS/DISCLOSURE

The potential for data loss does not only apply to portable media it also applies to any data which is:

- Transmitted over a network and reaching an unintended, unauthorized - recipient (such as the use of e-mail to send sensitive data)
- Intercepted over the internet through non secure channels
- Posting of data on the internet whether accidental or intentional
- Published on the company's website and identified as inaccurate or inappropriate (which must be reported)
- Conversationally – information disclosed during conversation
- Press or media – unauthorized disclosure by employees or an ill advised representative to the press or media
- Data which can no longer be located and is unaccounted for on an IT system
- Paper copies of data and information which can no longer be located
- Hard copies of information and data accessible from desks and unattended areas

All company employees, partner agencies, contractors and vendors must act responsibly, professionally and be mindful of the importance of maintaining the security and integrity of company data at all times.

Any loss of data and/or disclosure whether intentional or accidental must be reported immediately to the concerned departments immediately.

PERSONAL INFORMATION ABUSE

All person identifiable information – i.e. information which can identify an individual such as home address, bank account details etc... must not be disclosed, discussed or passed on to any person/s who is not in a position of authority to view, disclose or distribute such information.
Any abuse/misuse of such person identifiable information must be reported.

PHYSICAL SECURITY

Maintaining the physical security of offices and rooms where data is stored, maintained, viewed or accessed is of paramount importance. Rooms or offices areas where secure information is located or stored must have a method of physically securing access to the room. Windows could also provide access to the room/office and must also be securely locked – particularly when the room is left unattended. Rooms which have not been secured should not be used to store sensitive and personal information and data - concerns about any rooms/office which should be securely locked or access restricted must be reported to the Transformation Service via the company Incident Reporting procedures.

LOGICAL SECURITY / ACCESS CONTROLS

Controlling, managing and restricting access to the Authority's Network, Databases and applications is an essential part of Information Security. It is necessary to ensure that only authorized employees can gain access to information which is processed and maintained electronically.

LOSS OR THEFT OF IT/INFORMATION

Data or information which can no longer be located or accounted for e.g. cannot be found in a location where it is expected to be, filing cabinet etc... or which is known/or suspected to have been stolen needs to be reported immediately to the management , IT Department , HR Department.

RESPONSIBILITIES

It is the responsibility for all Council employees, members, partner agencies, contractors and vendors who undertake work for the company, on or off the premises to be proactive in the reporting of security incidents. It is also a responsibility of all individuals and handlers of company data and information to ensure that all policies and procedures dealing with the security and integrity of information and data are followed. Regular security updates will be given out/mailed to all the employees whenever required by all the Department HO, if necessary.

BREACHES OF POLICY

Breaches of this policy and/or security incidents are incidents which could have, or have resulted in, loss or damage to company assets, including IT equipment and information, or conduct which is in breach of the company security procedures and policies.

All company employees, elected members, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible. This obligation also extends to any external organization contracted to support or access the Information Systems of the Council. In the case of third party vendors, consultants or contractors non-compliance could result in the immediate removal of access to the system

APPROVAL AUTHORITY AND REVIEW POLICY:

This policy is approved by the Board of VARDHAMAN CAPITAL PVT LTD This policy may be reviewed as and when there are any changes introduced by any statutory authority or as and when it is found necessary to change the policy due to business needs.

POLICY COMMUNICATION:

A copy of this policy shall be made available to all the relevant staff/persons such as: compliance officer / department in-charge /authorized persons.
Further, a copy of this policy has to be displayed on our website.